manjingliu的编程之旅

在校大学生，认真学编程

转 用Wireshark简单分析HTTPS传输过程-抓包过程

2015-11-16 12:25 1938人阅读 评论(0) 收藏 举报

分类：

安全（38）

实验环境：

操作系统：Kali linux 1.06 64位

软件：Wireshark

实验目的：查看https的协议传输过程。

一、打开软件，

二、打开后，选择菜单下的edit的Prefenrces，选择protocols下的ssl（因为我们要观测的是https的传输过程），点击开始：

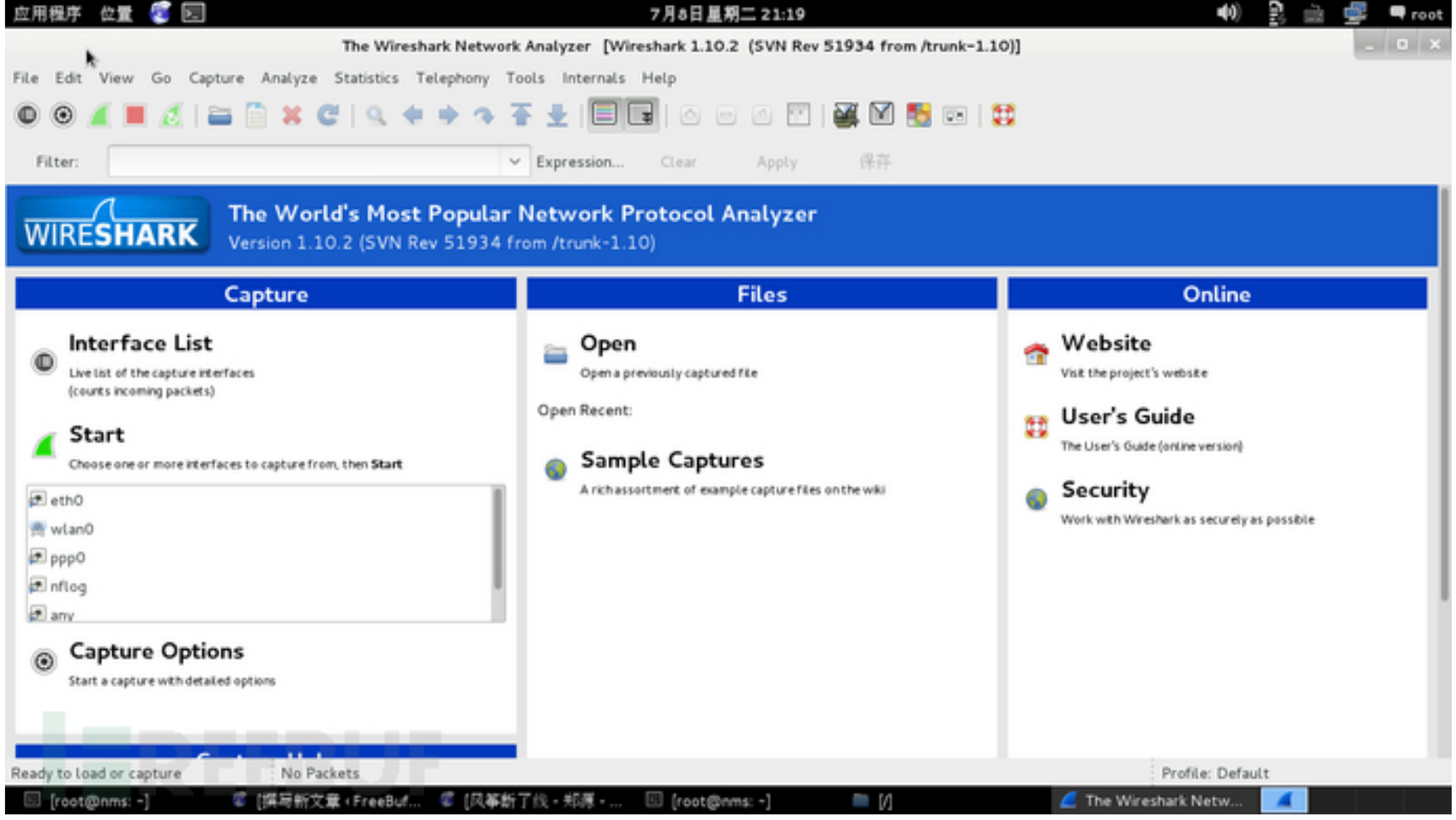
个人资料

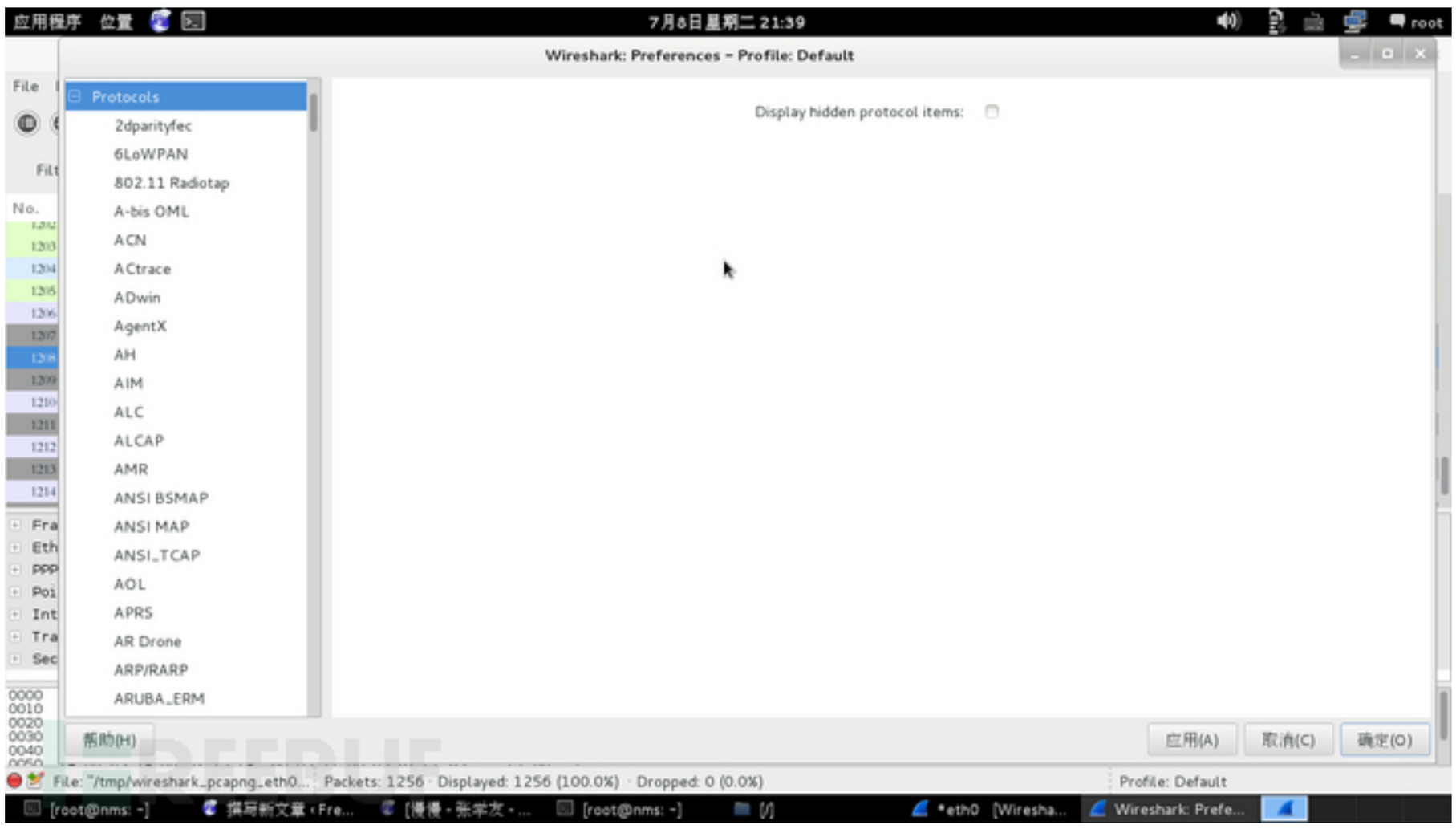
manjingliu

+ 加关注 发私信

访问： 76494次
积分： 1241
等级： BLOG 4
排名： 千里之外

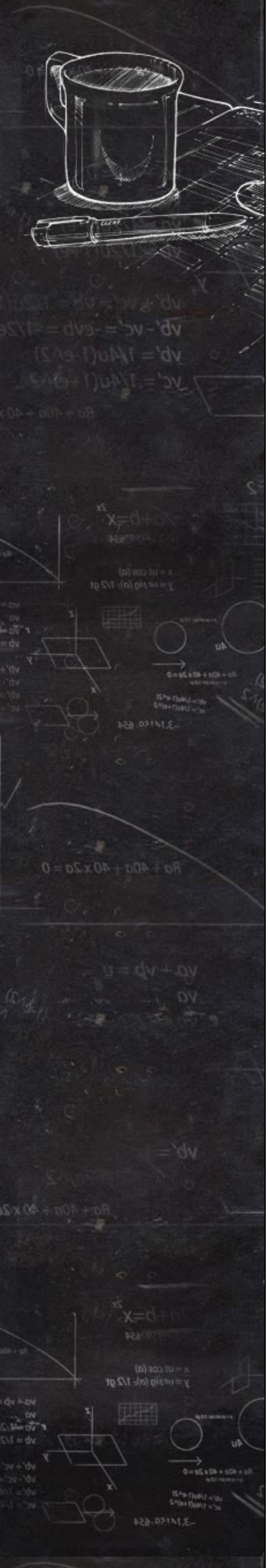
原创： 15篇 转载： 221篇
译文： 1篇 评论： 1条

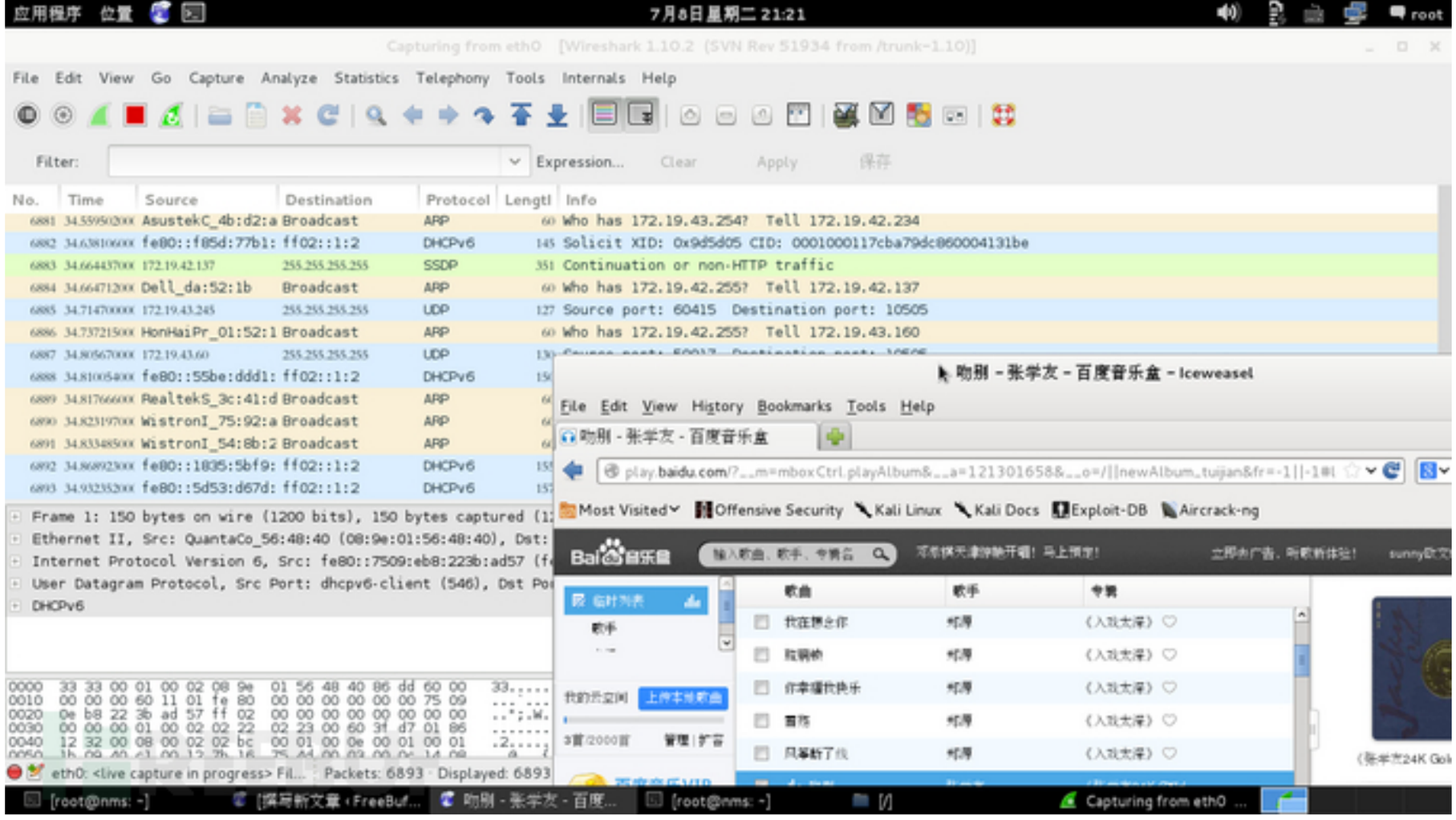




三、开始监听https传输数据：

因为我在放歌，所以看见数据传输很快哦，眨眼之间数据就跳走了：





回到正题，进入https站点，开始实践：

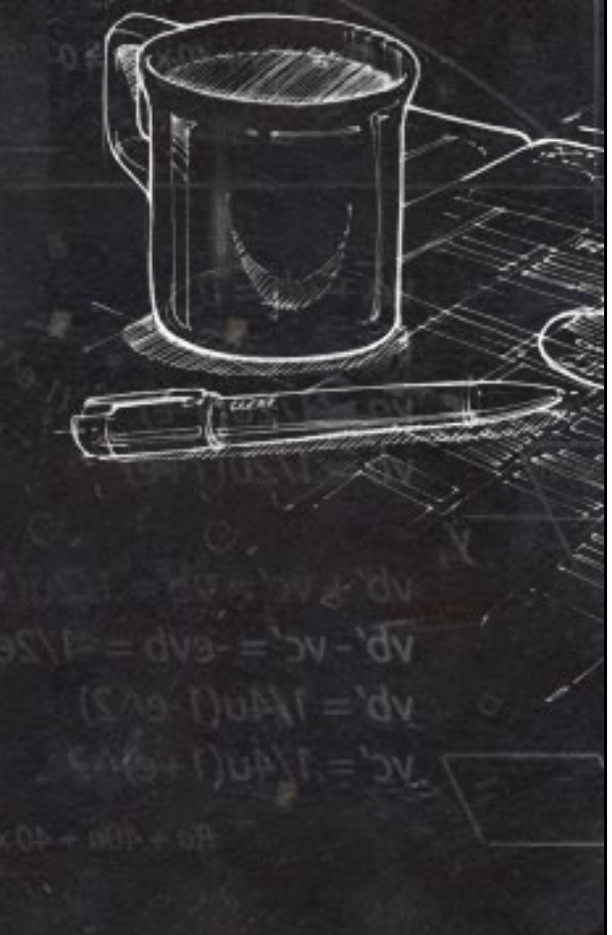
四、查看协议传输过程，（PS：Https=http+ssl）

1、 看见TLSv1了么?

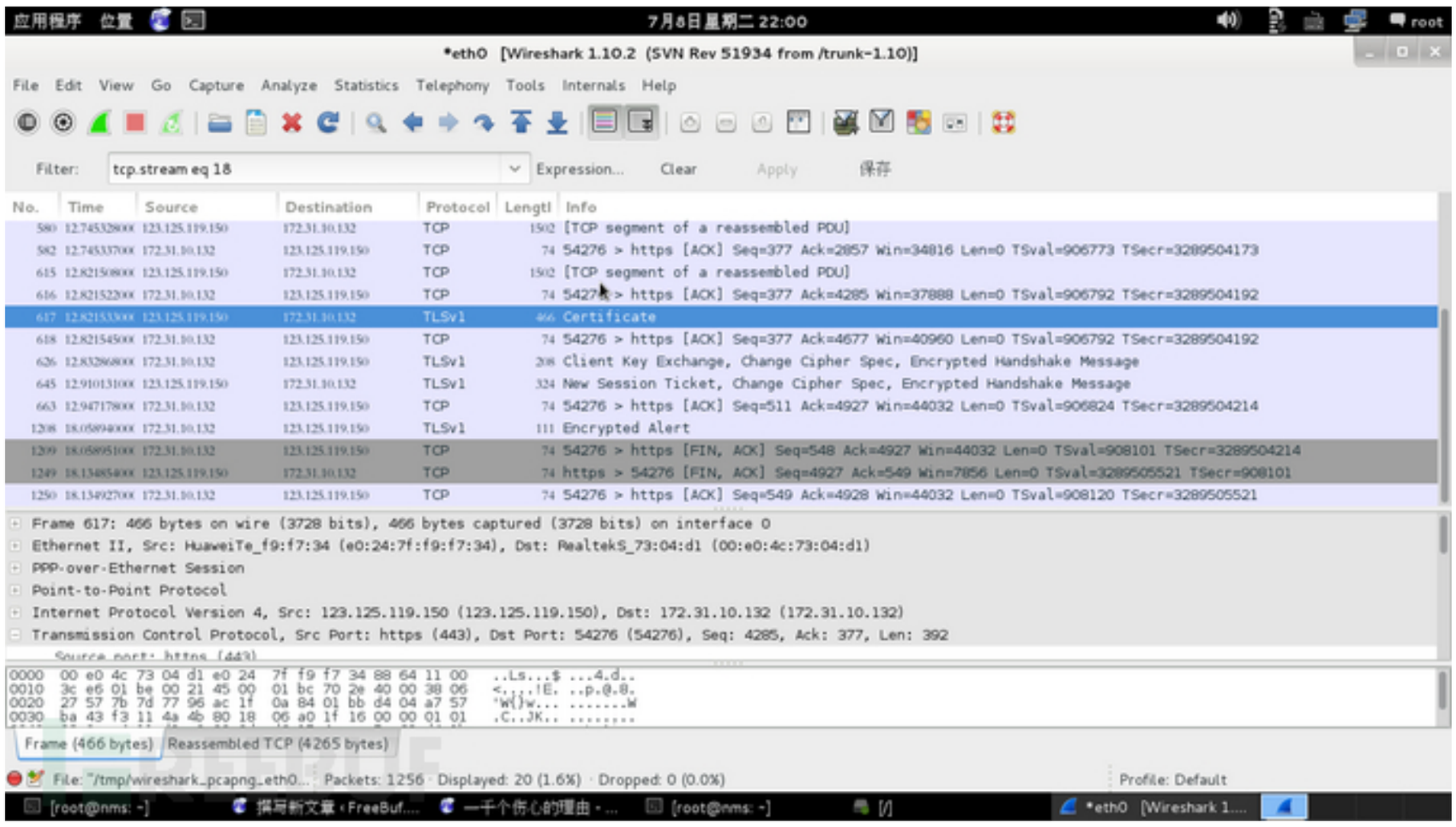
第一个就是蓝色就是我们PC电脑端向服务器发送HELLO，即浏览器向服务器请求一个安全的网页。

然后双击这个HELLO看下传输的内容：

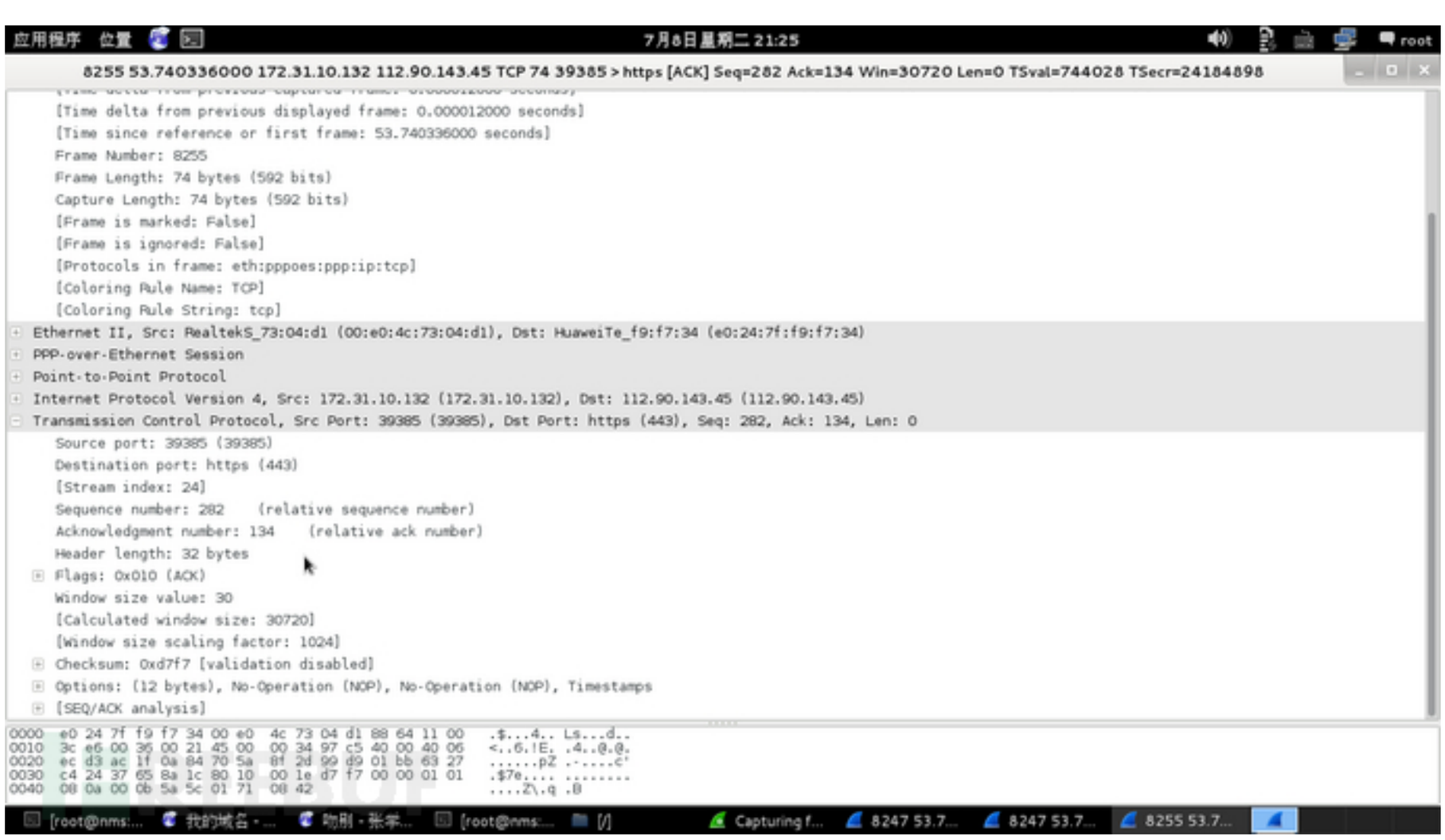
2、服务器就把它的证书和公匙发回来，同时向服务端发送ACK报文以便服务端确认数据是否无误。



3、服务端发送一句：“你好”，这是服务端知道那个请求是你发送的（同时它也会发送ACK报文确认发给你数据是否无误），同时浏览器会检查证书是不是由可以信赖的机构颁发的，确认证书有效和此证书是此网站的。



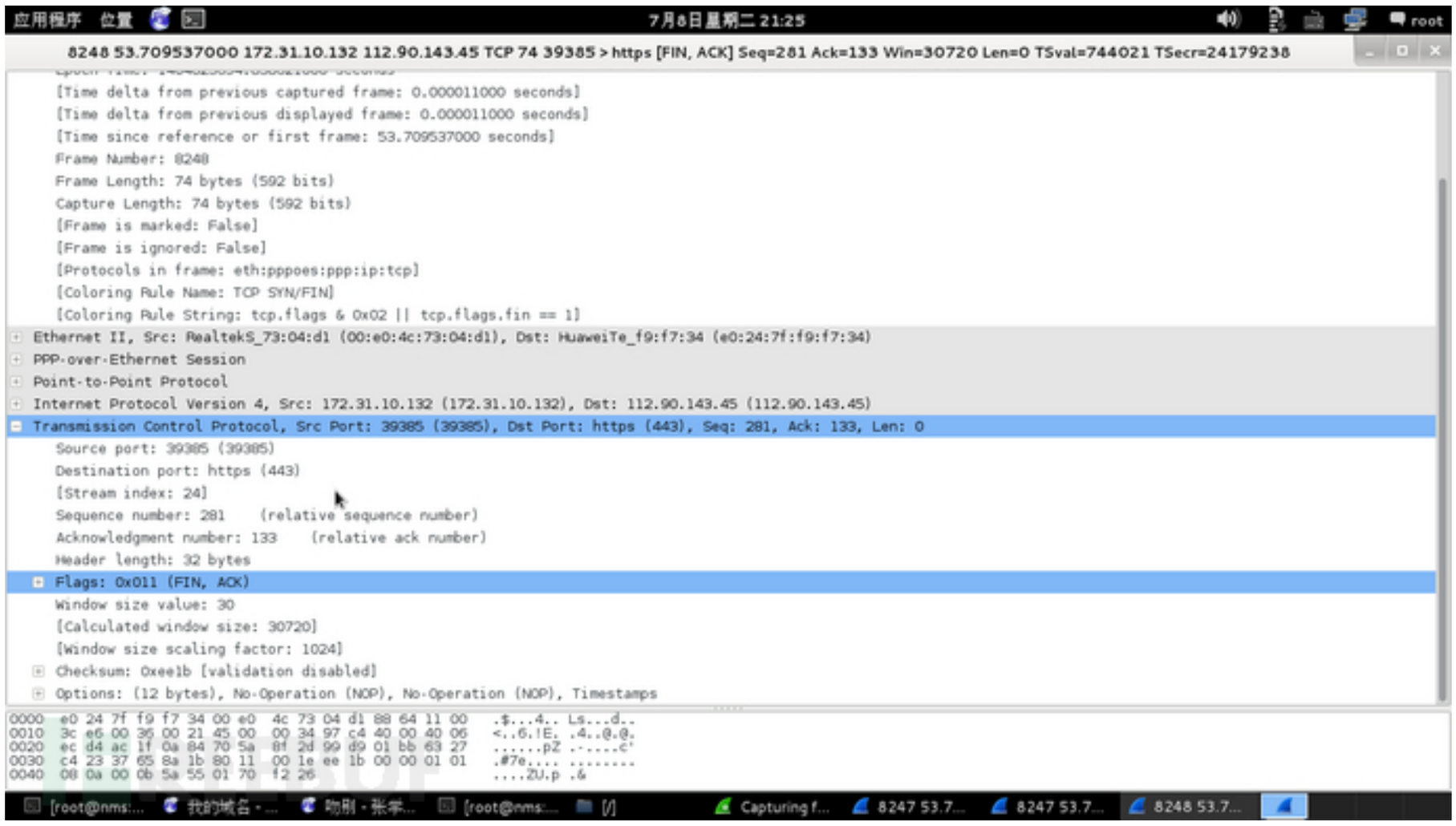
4、浏览器使用公钥加密了一个随机对称密钥，包括加密的URL一起发送到服务器

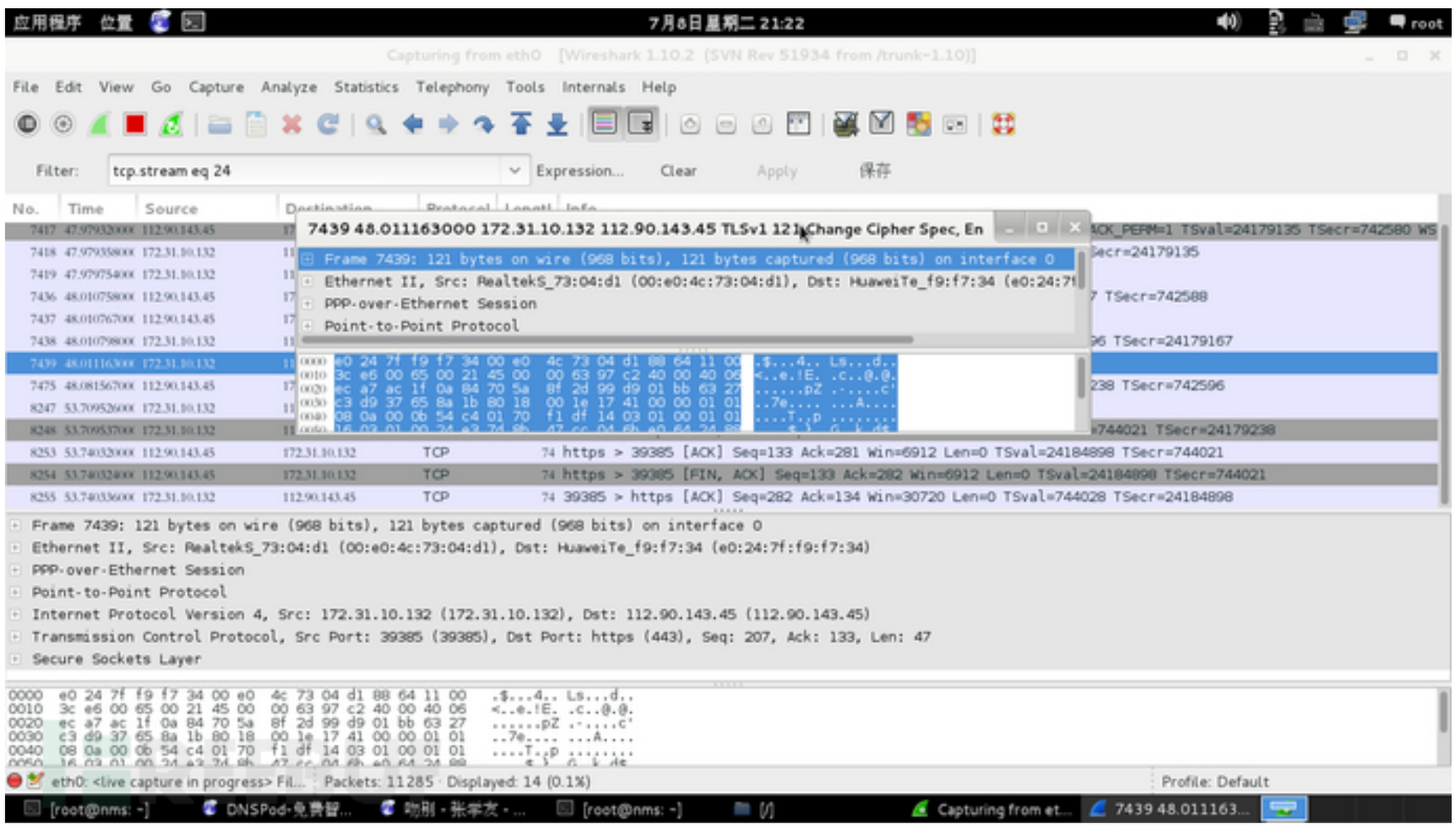


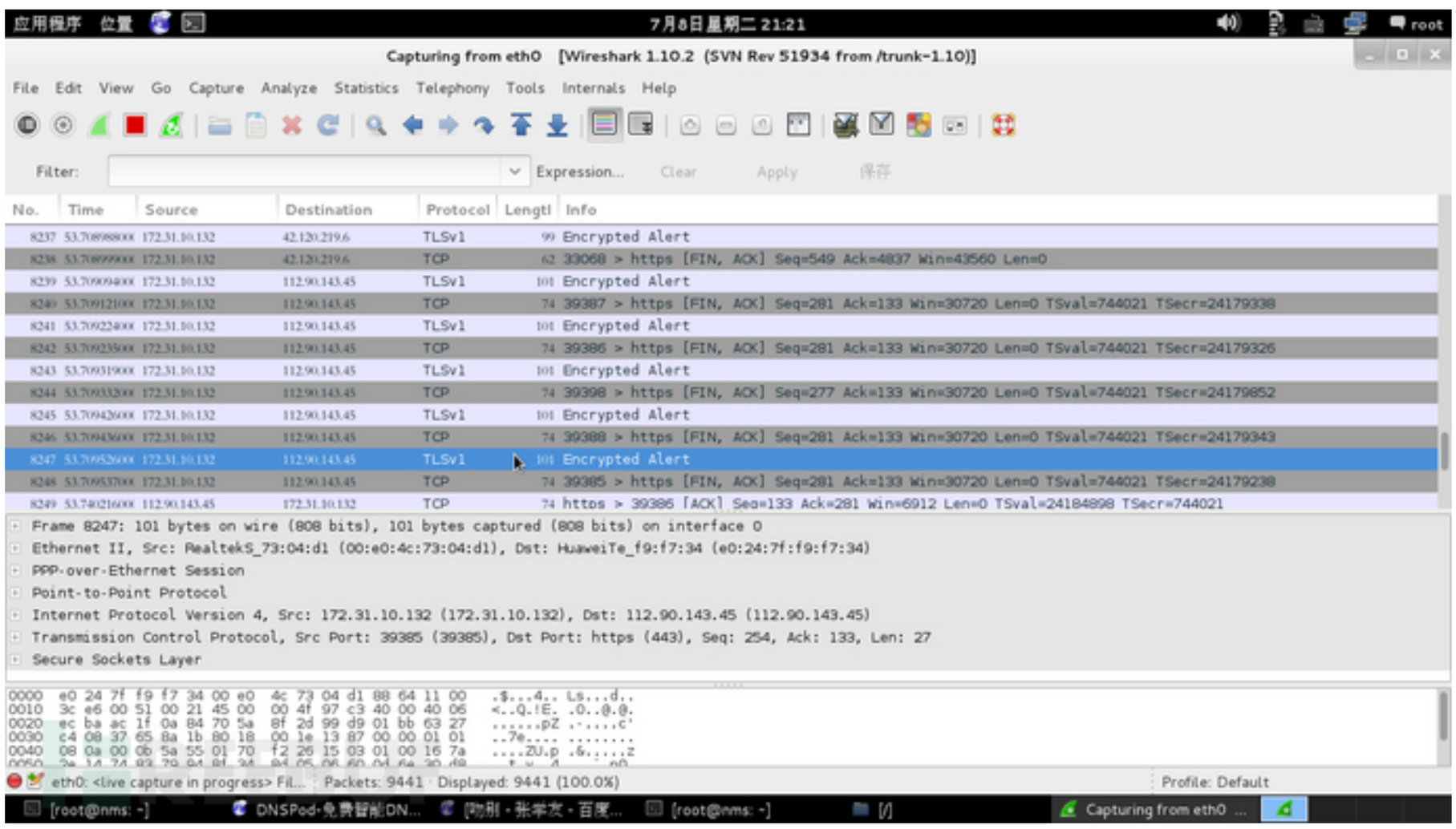
然后就是浏览器与服务器的交互过程：

1、服务器用自己的私匙解密了你发送的钥匙。然后用这把对称加密的钥匙给你请求的URL链接解密。

2、服务器用你发的对称钥匙给你请求的网页加密。你也有相同的钥匙就可以解密发回来的网页了。







文章写到这就应该结束了，本文写的不是很完善，主要是写个大概过程，写得不好的地方敬请大家多谅

解，本文主要是希望研究这方面的小伙伴能互相学习下。

顶 0　踩 0

上一篇 理解SSL（https）中的对称加密与非对称加密

下一篇 一次完整的HTTP请求所经历的7个步骤

相关文章推荐

- tcpdump抓取HTTP包
- Python全栈工程师特训班--韦玮
- tcpdump非常实用的抓包实例
- Blink在阿里集团的应用实践--陈守元
- https（ssl）协议以及wireshark抓包分析与解密
- Vue2.x知识点面面通
- 用Wireshark简单分析HTTPS传输过程-抓包过程
- 大型Web构架设计案例解析
- Wireshark抓包分析TCP的建立与断开过程
- 机器学习案例实战--欺诈检测
- Wireshark抓包分析TCP的建立与断开过程分析
- Android开发实战30分钟集成第三方SDK
- wireshark抓包tcp连接百度通信过程
- https访问github.com的Wireshark抓包文件
- wireshark https 抓包
- HTTPS--使用wireshark观察SSL/TLS握手过程--双…

查看评论

暂无评论

您还没有登录,请[登录]或[注册]

* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场

公司简介 | 招贤纳士 | 广告服务 | 联系方式 | 版权声明 | 法律顾问 | 问题报告 | 合作伙伴 | 论坛反馈

网站客服 杂志客服 微博客服 webmaster@csdn.net 400-660-0108 | 北京创新乐知信息技术有限公司 版权所有 | 江苏知之为计算机有限公司 |

江苏乐知网络技术有限公司

京 ICP 证 09002463 号 | Copyright © 1999-2017, CSDN.NET, All Rights Reserved